SECRET//NOFORN

Report No. DODIG-2015-048

INSPECTOR GENERAL

U.S. Department of Defense

December 8, 2014

(U//FOUO) Joint Cyber Centers

CENTCOM, (b)(1), 17(e), DoD OIG (b)(7)(E)

Cyberspace Operations

Classified by: Carol N. Gorman, Assistant Inspector General
Derived From: Multiple Sources
Declassify On: 20390529

Second Printing
Report 7 of 25

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

SECRET//NOFORN

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline 800 424 9098

For more information about whistleblower protection, please see the inside back cover.

~~SECRET//NOFORN~~

Results in Brief

(U//~~FOUO~~) Joint Cyber Centers

Cyberspace Operations

December 8, 2014

(U) Objective

(U) We determined whether Combatant Commands had sufficient cyber personnel and support from U.S. Cyber Command (USCYBERCOM) to effectively conduct cyber operations in their areas of operations.

(U) Finding

(U//~~FOUO~~) Combatant commanders made progress in implementing a command and control structure for cyberspace operations; however, additional actions are needed. Additionally, U.S. Pacific Command (USPACOM) and U.S. Central Command (USCENTCOM) in their Joint Cyber Centers and Cyber Support Element (CSE) support from USCYBERCOM to directed by the Joint Staff for planning, integrating, and synchronizing cyberspace operations. Specifically:

- (~~S~~) USPACOM Joint Cyber Center personnel of the tasks and were of the tasks;
- (U//~~FOUO~~) USCENTCOM Joint Cyber Center personnel of the tasks and were of the tasks; and
- (U//~~FOUO~~) USCYBERCOM did not consistently provide at USPACOM and at USCENTCOM.

(~~S//REL TO USA, FVEY~~) This occurred because previously validated and approved based on new cyber requirements; DoD

(U) Finding (cont'd)

(~~S//REL TO USA, FVEY~~) prioritized implementing and fielding the Cyber Mission Forces; and USCYBERCOM's temporary solution to task Service Component while fielding Cyber Mission Forces. As a result, offensive, defensive, and DoD Information Network cyberspace operations on cyberspace capabilities to execute missions.

(U) Recommendations

(U) We recommend that the Director, Joint Staff develop a communications strategy for disseminating incremental decisions and needed guidance. We also recommend that all combatant commanders conduct a command-wide, mission-impact analysis of cyberspace mission requirements, needed resources, and capability gaps affecting their ability to effectively implement command and control of cyberspace operations. Furthermore, we recommend that the Commanders, U.S. Strategic Command and USCYBERCOM increase CSE staffing at Combatant Commands cyberspace operations.

(U) Management Comments and Our Response

(U) We did not receive comments from the Commanders, USPACOM; U.S. European Command; U.S. Southern Command; U.S. Special Operations Command; U.S. Transportation Command; U.S. Strategic Command; U.S. Northern Command; and U.S. Africa Command, in response to the draft report. We revised recommendations based on management comments. Comments from USCYBERCOM and USCENTCOM partially addressed the recommendations, but further comments are required. Additionally, comments from the Joint Staff did not address the specifics of the recommendations. We request management comment on the final report by January 8, 2015. Please see the Recommendations Table on the back of this page.

(U) Recommendations Table

Unclassified Management	Recommendations Requiring Comments	No Additional Comments Required
Commander, U.S. Pacific Command Commander, U.S. European Command Commander, U.S. Southern Command Commander, U.S. Central Command Commander, U.S. Special Operations Command Commander, U.S. Transportation Command Commander, U.S. Strategic Command Commander, U.S. Northern Command Commander, U.S. Africa Command	2	
Commander, U.S. Strategic Command Commander, U.S. Cyber Command	3	
Director, Joint Staff	1	

Unclassified

(U) Please provide Management Comments by January 8, 2015.

~~SECRET//NOFORN~~

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANORIA, VIRGINIA 22350-1500

December 8, 2014

(U) MEMORANDUM FOR DISTRI8UTION

(U) SUBJECT: Joint Cyber Centers [redacted] Cyberspace Dperations (U//~~FOUO~~) (Report No. DODIG-2015-048)

(~~S//REL TO USA, FVEY~~) We are providing this report for review and comment. Combatant commanders made progress in implementing a command and control structure for cyberspace operations; however, further actions and resources are needed to [redacted] that do not exist within the other warfighting domains. In particular, U.S. Pacific Command and U.S. Central Command, which are recognized within DoD as having more mature cyberspace capabilities, [redacted] support from U.S. Cyber Command to [redacted] cyberspace operations.

(U) We considered management comments on a draft of this report when preparing the final report. However, the Commanders, U.S. Pacific Command; U.S. European Command; U.S. Southern Command; U.S. Special Dperations Command; U.S. Transportation Command; U.S. Strategic Command; U.S. Northern Command; and U.S. Africa Command did not comment on Recommendation 2, and the Commander, U.S. Strategic Command, did not comment on Recommendation 3. DoD Directive 7650.3 requires that recommendations be resolved promptly. Therefore, we request that the commanders provide comments on the finding and recommendations by January 8, 2015.

(U) As a result of management comments, we revised Recommendations 2 and 3. The Vice Director, Joint Staff, responding for the Director, Joint Staff, did not address the specifics of Recommendation 1. The Chief, Manpower Division, J1, responding for the Commander, U.S. Central Command, partially addressed the specifics of Recommendation 2. The Deputy Commander, USCYBERCOM, responding for the Commander, USCYBERCOM, partially addressed the specifics of Recommendation 3. We request that the Director, Joint Staff; the Commander, U.S. Central Command; and the Commander, U.S. Cyber Command, provide additional comments on the final report by January 8, 2015. Although not required to comment, the Director, Cost Assessment and Program Evaluation, agreed with the finding.

(U) Please provide comments that conform to the requirements of DoD Directive 7650.3. Classified comments must be sent electronically over the SECRET Internet Protocol Router Network (SIPRNET). Please send a PDF file containing your comments to [redacted] and [redacted] Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. Comments provided on the report must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01. If you consider any matters to be exempt from public release, you should mark them clearly for Inspector General consideration.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) DISTRIBUTION:

(U) UNDER SECRETARY OF DEFENSE FOR PDLICY
(U) COMMANDER, U.S. PACIFIC CDMMAND
(U) CDMMANDER, U.S. EUROPEAN COMMAND
(U) COMMANDER, U.S. SDUTHERN CDMMAND
(U) CDMMANDER, U.S. CENTRAL CDMMAND
(U) CDMMANDER, U.S. SPECIAL OPERATIONS COMMAND
(U) CDMMANDER, U.S. TRANSPDRTATIDN CDMMAND
(U) CDMMANDER, U.S. STRATEGIC COMMAND
(U) COMMANDER, U.S. CYBER CDMMAND
(U) COMMANDER, U.S. NDRTHERN CDMMAND
(U) COMMANDER, U.S. AFRICA COMMAND
(U) DIRECTDR, JDINT STAFF
(U) DOD CHIEF INFORMATION DFFICER
(U) DIRECTOR, COST ASSESSMENT AND PRDGRAM EVALUATIDN

(U) Contents

(U) Introduction

(U) Objective

(U) Our objective was to determine whether Combatant Commands had sufficient cyber personnel and support from U.S. Cyber Command (USCYBERCOM) to effectively conduct cyber operations in their areas of operations. [See Appendix A for the scope and methodology and prior audit coverage related to the objective.]

(U) Background on DoD Cyberspace Operations

(U//~~FOUO~~) DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control (C2) of the full spectrum of military operations. Cyberspace is one of the five DoD domains; the other domains are air, land, maritime, and space. Cyberspace, unlike the other physical domains, is a global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations employ cyberspace capabilities to ensure access and freedom of operations in, through, and from cyberspace to deliver effects in any of the domains at times and places of DoD's choosing; to deny adversaries access and freedom of operations at times and places of DoD's choosing; and to sustain mission-essential segments of cyberspace (networks) in the face of adversary action or stressed environments.

(U//~~FOUO~~) Cyberspace operations are categorized under three lines of operations based on their intent:

1. (U//~~FOUO~~) **Offensive Cyberspace Operations.** Project power by the application of force in and through cyberspace.
2. (U//~~FOUO~~) **Defensive Cyberspace Operations.** Defend DoD or other friendly cyberspace.

3. (U//~~FOUO~~) **DoD Information Network (DoDIN) Dperations.** Design, build, configure, secure, operate, maintain, and sustain DoD communications systems and networks to create and preserve data availability, integrity, confidentiality, as well as user authentication and nonrepudiation.[1]

(U) Cyberspace Responsibilities and Requirements

(U//~~FOUO~~) Under the authority of the Secretary of Defense, DoD uses cyberspace capabilities to perform integrated offensive and defensive operations. The Deputy Assistant Secretary of Defense for Cyber Policy, Office of the Under Secretary of Defense for Policy, integrates cyberspace operations into national and DoD strategies, develops policy related to cyber forces and employment of those forces, and ensures cyber capabilities are integrated into operation and contingency plans. The Chairman of the Joint Chiefs of Staff ensures cyberspace plans and operations are compatible with other military plans. Although the Commander, U.S. Strategic Command (USSTRATCOM) is responsible for securing, operating, and defending the DoDIN, and critical cyberspace assets, systems, and functions against an intrusion or attack, the Commander delegated most cyberspace responsibilities to the Commander, USCYBERCOM. The Commander, USCYBERCOM has three mission areas: defend the Nation against strategic cyber attacks; support Combatant Command contingency and operational planning; and support the security, operation, and defense of the DoDIN.

(U//~~FOUO~~) The other combatant commanders operate and defend their tactical and constructed networks and integrate cyberspace capabilities into all military operations. As such, combatant commanders have responsibility for integrating cyberspace capabilities into their command plans and coordinating with other combatant commanders, the Military Services, and DoD agencies to create fully integrated capabilities. The Military Services support combatant commanders by organizing, training, and equipping forces in addition to securing and defending their global networks.

(U//~~FOUO~~) Du May 1, 2012, the Secretary of Defense issued a memorandum, "Transitional Framework for Cyberspace Dperations Command and Control (C2)," directing combatant commanders to establish Joint Cyber Centers (JCCs) using existing capabilities and personnel to standardize C2 of cyberspace operations based on the

[1] (U//~~FOUO~~) Nonrepudiation is assurance the sender of data receives proof of delivery and the recipient receives proof of the sender's identify to prevent either from later denying they processed the data.

(U//~~FOUO~~) March 15, 2012, Joint Staff Transitional Cyberspace Operations C2 Concept of Operations. [See Appendix B for a timeline of critical cyberspace events related to combatant commanders establishing JCCs and taking responsibility for planning and integrating cyberspace into operations.] The Transitional Cyberspace Operations C2 Concept of Operations requires USSTRATCOM and USCYBERCOM to directly support JCC operations through forward-deployed Cyber Support Elements (CSEs).[2] Additionally, it requires JCCs to perform 41 cyberspace tasks related to coordinating, planning, synchronizing, and deconflicting Combatant Command cyberspace operational requirements. It also requires combatant commanders to perform 24-unique cyberspace tasks but does not specify that the JCCs are responsible for performing these tasks. At U.S. Pacific Command (USPACOM), [redacted] whereas the JCC at U.S. Central Command (USCENTCOM) was [redacted].[3] [See Appendix C for the list of 65 cyberspace tasks directed by the Joint Staff.] Joint Publication 3-12, "Cyberspace Operations," February 5, 2013, requires USCYBERCOM CSEs to provide JCCs with reachback[4] capabilities and support from USCYBERCOM and the Service Components. The Joint Staff Transitional Cyberspace Operations C2 Concept of Operations requires CSEs to perform six-unique tasks to support JCCs in planning and integrating cyberspace into command operations.

(~~S//REL TO USA, FVEY~~) The Chairman of the Joint Chiefs of Staff issued an "Execute Order to Implement Cyberspace Operations C2 Framework," June 21, 2013, (Execute Order) [redacted]

[2] (U//~~FOUO~~) CSEs are cyberspace operations planners and subject matter experts.

[3] (U//~~FOUO~~) USCENTCOM's analysis of its JCC's ability to complete cyberspace tasks was based only on 60 of the 65 Joint Staff–directed tasks because other USCENTCOM joint directorates were responsible for the 5 tasks.

[4] (U//~~FOUO~~) Reachback is performed by the CSEs, as USCYBERCOM experts, to facilitate communication with USCYBERCOM to enable coordination, deconfliction, and synchronization of supporting USCYBERCOM effects as requested by the Combatant Commands.

Introduction

~~(S//REL TO USA, FVEY)~~ [redacted]

~~(S//REL TO USA, FVEY)~~ *Figure 1:* [redacted]

(U) Source: USCYBERCOM

(U//~~FOUO~~) USCYBERCOM documentation defines the [redacted] at the operational level of warfare with a matrixed-staff organization planning and executing military cyberspace operations. The primary difference between the two models is that the operational control model gives combatant commanders operational control over specific Combat Mission Forces (Combat Mission Teams and Combat Support Teams). The Joint Staff acknowledged that all Combatant Commands would not implement the operational control model because of differences in each command's cyberspace mission. Figure 2 on the next page describes the future C2 operational structure.

~~(S//REL TO USA, FVEY)~~ Figure 2: [redacted]

(U) Source: USCYBERCOM

~~(S//REL TO USA, FVEY)~~ The Cyber Mission Forces are composed of [redacted] In total, DoD plans to dedicate approximately [redacted]. Throughout FY 2014, USCYBERCOM and the Service Components fielded [redacted] Table 1 on the next page identifies the composition and missions of the [redacted] teams and the number of teams and personnel comprising each team.

~~(S//REL TO USA, FVEY)~~ Table 1. Composition of the [redacted] Teoms

*(U//~~FOUO~~) The Execute Order directs combatant commanders, upon initial operating capability, to assume operational control over Combatant Command Cyber Protection Teams.

(U) Review of Internal Controls

(U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that internal controls are operating as intended and to evaluate the effectiveness of the controls. We did not find internal control weaknesses at USPACOM, USCENTCOM, or USCYBERCOM related to our audit objective. Although we did not identify any internal control weaknesses, we found deficiencies at USPACDM, USCENTCDM, and USCYBERCDM that affected the commands' ability to effectively plan and integrate cyberspace into command plans and operations.

(U) Finding

(U//~~FOUO~~) Resources Needed to Effectively Plan and Integrate Combatant Command Cyberspace Operations

(U//~~FOUO~~) Combatant commanders made progress in implementing a C2 structure for cyberspace operations by establishing JCCs and integrating CSEs into daily operations. However, additional actions are needed in a resource-constrained environment to enable combatant commanders to effectively plan and integrate cyberspace into operations.

(U//~~FOUO~~) In addition, USPACOM and USCENTCOM [redacted] and CSE support from USCYBERCOM[5] to [redacted] directed by the Joint Staff for planning, integrating, and synchronizing cyberspace operations. Specifically:

- (~~S~~) USPACOM JCC personnel [redacted], and were [redacted] of the tasks;
- (U//~~FOUO~~) USCENTCOM JCC personnel complete [redacted] of the tasks, and were [redacted] of the tasks; and
- (U//~~FOUO~~) USCYBERCOM [redacted] CSEs at USPACOM and at USCENTCOM [redacted] the CSEs to effectively [redacted] tasks and to support JCC cyberspace operations.

[5] (U//~~FOUO~~) Although the Execute Order and Transitional Cyberspace Operations C2 Concept of Operations directed USSTRATCOM and USCYBERCOM to provide CSEs, we focused on USCYBERCOM because it requested permanent billets and issued task orders to meet this requirement.

[6] (U//~~FOUO~~) USCENTCOM officials stated other joint directorates and not the JCC [redacted]. We did not assess whether the joint directorates completed these tasks.

Finding

(U) This occurred because:

- (U//~~FOUO~~) previously validated and approved [redacted] to support the fielding of [redacted] Forces and changes to the cyberspace environment;
- (U//~~FOUO~~) DoD prioritized the implementation and fielding of the [redacted] Forces; and
- (~~S//REL TO USA, FVEY~~) USCYBERCOM's [redacted]

(~~S//REL TO USA, FVEY~~) As a result, USPACOM and USCENTCOM have [redacted] capabilities into [redacted] operations and command plans, [redacted] to execute the combatant commanders' missions. Specifically, USPACOM JCC personnel [redacted] operational and contingency plans, while USCENTCOM personnel have [redacted] plans.

(U) Progress Made in Implementing the Transitional Cyberspace Operations C2 Concept of Operations

(~~S//NF~~) Combatant commanders made progress in implementing the Joint Staff Transitional Cyberspace Operations C2 Concept of Operations [redacted]

(U//~~FOUO~~) Combatant commanders made progress in implementing the Joint Staff Transitional Cyberspace Operations C2 Concept of Operations.

[redacted] Additionally, the

(S//NF) [redacted]

(U//~~FOUO~~) Since establishing the JCCs, USPACOM and USCENTCOM began planning, directing, and synchronizing cyberspace operations with support from forward-deployed CSEs. Specifically, they began focusing on cyberspace situational awareness and incorporating cyberspace into their operational and contingency plans; exercises; and boards, bureaus, centers, cells, and working groups.[7] For example, the Director, J6 (Command, Control, Communications, and Cyber) requires daily reporting and weekly cyber update briefings from all components and forces in the USPACOM theater to synchronize cyberspace operations and to provide the Commander, USPACOM continuous situational awareness of cyberspace issues and threats affecting the command. Further, the USPACOM and USCENTCOM JCCs began developing or expanding cyberspace partnerships with allies, international partners, and other Governmental agencies in their areas of operation. For example, USCENTCOM issues threat warnings to regional partners about their critical infrastructure and key resources [redacted]

(U//~~FOUO~~) While DoD made progress in implementing command structures for executing the new cyber mission, additional actions are needed in a resource-constrained environment to enable all Combatant Commands to effectively plan and integrate cyberspace into operations. USPACOM and USCENTCOM officials stated that although they generally shared information between the commands pertaining to their progress in implementing the direct support model (JCC and CSE construct), they did not regularly communicate similar information with other Combatant Command JCC personnel. Officials from the Joint Staff acknowledged that the [redacted]. In addition, Joint Staff officials also acknowledged that Combatant Commands were not effectively

(U//FOUO) Additional actions are needed in a resource-constrained environment

[7] (U) Boards, bureaus, centers, cells, and working groups include cross-functional experts (for example, representation from multiple joint directorates with a stake in a particular mission or task) within a Combatant Command brought together to facilitate, coordinate, plan, and execute specific missions and tasks.

Finding

(U//~~FOUO~~) communicating with each other [redacted] mission. [redacted]

(U//~~FOUO~~) Additionally, USPACOM and USCENTCOM officials identified the need for further guidance and information from the Joint Staff to assist them in planning and integrating cyberspace into operations based on the rapidly changing cyberspace domain. For example, USPACOM officials stated that additional information to better understand the genesis of cyberspace decisions affecting Combatant Commands, and guidance identifying Combatant Command authorities for planning and executing operations and sharing information with partners was needed. Additionally, USCENTCOM officials stated that guidance was needed for integrating the JCCs and CSEs, and for prioritizing and responding to Combatant Command threats. Furthermore, USCENTCOM officials stated [redacted] to incorporate lessons learned from the commands that implemented JCCs to better enable the commands to identify needed JCC resources.

(U//~~FOUO~~) Not regularly sharing information or providing timely guidance and decisions decreased the combatant commanders' ability to effectively plan and prioritize cyberspace operations in a resource-constrained and rapidly evolving domain. The Joint Staff and the Commander, USCYBERCOM could consider conducting regular global synchronization conferences as part of their strategy for improving communication. Additionally, the Joint Staff, in coordination with USSTRATCOM, could consider updating the Transitional Cyberspace Operations C2 Concept of Operations or issuing an updated Execute Order or fragmentary order to provide more timely guidance. The Director, Joint Staff should develop a communications strategy for disseminating incremental decisions and timely guidance affecting cyberspace command and control until the end-state for command and control of cyberspace operations is defined and achieved.

(U) [redacted] Personnel to Perform Cyberspace Tasks

~~(S//REL TO USA, FVEY)~~ [redacted]

(U) Adequately resourcing the JCC mission has been and continues to be a challenge.

[redacted]

(U//~~FOUO~~) USPACOM [redacted] Integrating Cyberspace Operations

~~(S)~~ [redacted]

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted];
- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted].

(S)

(U//~~FOUO~~) In 2012, USPACOM established its JCC using personnel from its J6 to accomplish the cyberspace tasks directed by the Joint Staff. In addition, the USPACOM J2 (Intelligence) and J3 (Operations) supported the JCC in performing the cyberspace tasks. The Director, J6, USPACOM recognized the need for additional staff. As a result, the Chief of Staff, USPACOM requested a comprehensive manpower and organizational evaluation of the missions, functions, and required capabilities of USPACOM based on factors such as the evolving national cyber mission. The results of that evaluation, which were completed in April 2013, showed USPACOM perform the core JCC functions.

(S//~~NF~~)

[8]

[8] (U) USPACOM would receive in FY 2015; in FY 2016; and in FY 2017.

Finding

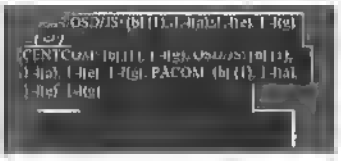
(U//FOUO) USPACOM officials acknowledged the previously validated [redacted]

(~~S//REL TO USA, FVEY~~) [redacted]

(S) [redacted]. In a

[9] (~~S//REL TO USA, FVEY~~) The [redacted] Teams.

Finding



(S//[redacted]

and the theater.

(U//~~FOUO~~) USCENTCOM [redacted] Integrating Cyberspace Operatians

(U//~~FOUO~~) USCENTCOM did [redacted] plan, coordinate, integrate, and synchronize cyberspace operations. Specifically, the USCENTCOM JCC [redacted] performing cyberspace operations as of May 2014. Although we requested, and the JCC Chief agreed to provide, an updated analysis of the JCCs ability to complete Joint Staff–directed tasks during the audit, USCENTCOM did not conduct that assessment. The most recent USCENTCOM assessment, which JCC personnel completed in February 2013 [redacted]. [See Appendix C for the list of 65 Joint Staff–directed tasks and USCENTCOM's status in completing the tasks.] Of significance, USCENTCOM did [redacted] complete essential functions to:

- (U//~~FOUO~~) conduct network mission assurance and critical cyberspace infrastructure protection analysis [redacted];
- (U//~~FOUO~~) identify critical networks [redacted];
- (U//~~FOUO~~) develop and integrate cyberspace operations [redacted]; and
- (U//~~FOUO~~) identify command cyberspace forces' readiness [redacted].

(S//REL TO USA, FVEY)

(U//~~FOUO~~) In August 2013, USCENTCOM als to the Joint Staff as a result of the JCCs .[10]

(S//REL TO USA, FVEY)

[10] (U)

[11] (S//REL TO USA, FVEY)

Finding

(~~S//REL TO USA, FVEY~~) The USCENTCOM JCC Chief also [redacted]. The USCENTCOM request for [redacted]. Although USCENTCOM has [redacted].

(U) Recurring [redacted] Personnel

(U) During 2012 and 2013, a Joint Staff J7 Joint and Coalition Operational Analysis team conducted an initial assessment of DoD's effectiveness in implementing the Secretary of Defense-directed transitional C2 framework. The Joint and Coalition Operational Analysis report, "Transitional Cyberspace Operations C2 Concept of Operations," July 15, 2013, [redacted]. The report found that JCCs used matrixed-organizational constructs, dual-hatted personnel, or augmentees to fill staffing shortages. [redacted].

(U) Combatant Command structures were inadequately resourced.

(U//~~FOUO~~) As previously reported, USPACOM and USCENTCOM [redacted]. In addition to their requests, U.S. Northern Command and U.S. Southern Command also [redacted]. For the FY 2016 Program Budget Review process, the Joint Staff provided documentation showing that seven of the nine Combatant Commands already submitted memorandums describing their

[12] (U) A targeteer supports Combatant Command cyber targeting processes to ensure targets are integrated into or deconflicted with plans and operations.

(U//~~FOUO~~) intent to [redacted]

(U//~~FOUO~~) Based on information obtained from USPACOM and USCENTCOM, in addition to the Joint and Coalition Operational Analysis findings and the Combatant Command [redacted]. Until each Combatant Command identifies all cyberspace requirements affecting its command and conducts a thorough analysis of JCC functions, [redacted], these challenges will continue to exist. Therefore, all combatant commanders should conduct a detailed, command-wide, mission-impact analysis to identify all cyberspace mission requirements and tasks, needed resources, and capability gaps affecting their ability to effectively implement C2 of cyberspace operations.

(U//~~FOUO~~) USCYBERCOM [redacted] CSE Requirements

(~~S//REL TO USA, FVEY~~) USCYBERCOM [redacted]

[13] (U//~~FOUO~~) The seven Combatant Commands are USPACOM, U.S. European Command, U.S. Northern Command, U.S. Transportation Command, U.S. Africa Command, U.S. Special Operations Command, and USSTRATCOM.

Finding

(S//~~REL TO USA, FVEY~~) [redacted]

(U//~~FOUO~~) The Joint Staff Transitional Cyberspace Operations C2 Concept of Operations requires CSE [redacted] support JCCs in completing their tasks. These tasks are:

1. (U//~~FOUO~~) [redacted]
2. (U//~~FOUO~~) [redacted]
3. (U//~~FOUO~~) [redacted]
4. (U//~~FOUO~~) [redacted]
5. (U//~~FOUO~~) [redacted]
6. (U//~~FOUO~~) [redacted]

[14] (U//~~FOUO~~) Liaison officers have primary responsibility for supporting designated Combatant Commands and facilitating and communicating command cyberspace requirements, issues, and command direction with USCYBERCOM.

(S//REL TO USA, FVEY)

(S//REL TO USA, FVEY)

(U//FOUO) USPACOM and USCENTCOM also relied on the CSEs to

(S//REL TO USA, FVEY)

[15] (U)

Finding

(S//~~REL TO USA, FVEY~~) [redacted]

(U//~~FOUO~~) While USCYBERCOM requested [redacted] through tasking orders, it also requested, and the Joint Staff validated, [redacted]. USCYBERCOM based its need for [redacted] and its internal assessment. [redacted]

(U//~~FOUO~~) Table 2 on the next page [redacted]

(U//~~FOUO~~) USCYBERCOM was providing [redacted] CSE personnel.

[redacted]. For example, the table shows USCYBERCOM was providing [redacted] personnel at USPACOM and USCENTCOM [redacted].

[16] (U//~~FOUO~~) The Joint Staff validated [redacted]

(U//~~FOUO~~) Table 2. CSE Support Provided to Combatant Commands

(U//~~FOUO~~) The Deputy's Management Action Group [redacted] because DoD prioritized implementing and fielding Cyber Mission Forces [redacted]. Although the reasons for the Deputy's Management Action Group decisions [redacted], the Director, Manpower and Personnel, USCYBERCOM; the Director, Command, Control, Communications, and Computers and Information Programs Division, Cost Assessment and Program Evaluation; and officials from the Joint Staff and Office of the Deputy Assistant Secretary of Defense for Cyber Policy stated that [redacted] USCYBERCOM's request did not clearly explain the differences between JCC and CSE functionality. Additionally, they stated that the request did not distinguish the forward-deployed positions from a growth in headquarters personnel. A May 2011 Government Accountability Office report[17] concluded that the Military Services may

(U//~~FOUO~~) [redacted] USCYBERCOM's request did not clearly explain the differences between JCC and CSE functionality.

[17] (U) Government Accountability Office Report 11-421, "More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 20, 2011.

Finding

(U//~~FOUO~~) have difficulty in meeting their personnel requirements in organizing, training, equipping, and providing cyber forces because of the limited DoD cyber workforce. We recognize the need to prioritize competing requirements in a resource-constrained environment. However, the Joint Staff

(S//~~REL TO USA, FVEY~~)

(S//~~REL TO USA, FVEY~~) to

(U//~~FOUO~~)
...USCYBERCOM has

[18] (U//~~FOUO~~) As of July 2014, USCYBERCOM provided liaison officers to all Combatant Commands with the exception of U.S. Africa Command.

~~(S//REL TO USA, FVEY)~~ [redacted]. The Commanders, USSTRATCOM and USCYBERCOM should [redacted] for [redacted].

(U//~~FOUO~~) Limited Reliance on Cyberspace Operations

~~(S//REL TO USA, FVEY)~~ Since the Secretary of Defense issued direction to standardize C2 of cyberspace operations in May 2012 by requiring combatant commanders to establish JCCs and for USCYBERCOM to provide CSEs, USPACOM and USCENTCOM began the process of institutionalizing cyberspace to meet Joint Staff guidance. [redacted]

~~(S//REL TO USA, FVEY)~~ [redacted]

Finding

~~(S//REL TO USA, FVEY)~~ [redacted]

~~(S//REL TO USA, FVEY)~~ [redacted]

(U) Conclusion

~~(S//REL TO USA, FVEY)~~ [redacted]

(S//REL TO USA, FVEY) [redacted]

(S//REL TO USA, FVEY) [redacted]

(U) Recommendations, Management Comments, and Our Response

(U) Revised Recommendations

(U//~~FOUO~~) As a result of management comments, we revised Recommendation 2 to ensure the detailed, command-wide, mission-impact analysis addressed not only cyberspace tasks included in the Transitional Cyberspace Operations C2 Concept of Operations, but also accounted for other cyberspace requirements and tasks affecting each Combatant Command. We also revised Recommendation 3 to clarify that [redacted]

Finding

(U) Recommendation 1

(U) We recommend that the Director, Joint Staff develop a communications strategy for disseminating incremental decisions and timely guidance affecting cyberspace command and control to facilitate cross Combatant Command information sharing and to allow the combatant commanders to effectively plan and prioritize cyberspace operations and integrate Cyber Mission Forces into operations until the end-state for command and control of cyberspace operations is defined and achieved for all Combatant Commands.

(U) Joint Staff Comments

(U//~~FOUO~~) The Vice Director, Joint Staff, responding for the Director, Joint Staff, agreed with the report.

(U) Our Response

(U) Although the Vice Director agreed with the report, he did not state agreement or disagreement with or address the specifics of the recommendation on a draft of this report. Therefore, we request that the Director, Joint Staff provide comments on the final report by January 8, 2015.

(U) Recommendation 2

(U) We recommend that the Commanders, U.S. Northern Command, U.S. Transportation Command, U.S. Pacific Command, U.S. Southern Command, U.S. Central Command, U.S. Africa Command, U.S. European Command, U.S. Strategic Command, and U.S. Special Operations Command conduct a detailed, command-wide, mission-impact analysis to identify all cyberspace mission requirements and tasks, needed resources, and capability gaps [redacted].

(U) USCENTCOM Comments

(U) The Chief, Manpower Division, J1, responding for the Commander, USCENTCOM, agreed, stating that USCENTCOM internally completed a mission-impact analysis [redacted].

(U) Our Response

(U//~~FOUO~~) Although the Chief, Manpower Division agreed, the comments partially addressed the specifics of the recommendation. The workload analysis did not meet the intent of performing a detailed, command-wide, mission-impact analysis. We acknowledge that initial external manpower studies were completed during 2012 and 2013. We also acknowledge that [redacted]. We requested an updated workload analysis during the audit to determine USCENTCOM's ability to complete cyberspace tasks directed by the Joint Staff and to determine whether USCENTCOM JCC personnel performed other tasks to complete additional cyberspace requirements. For example, the 2013 Execute Order includes additional cyberspace requirements related to achieving operational control over specific Cyber Mission Forces. However, USCENTCOM did not provide further documentation showing that the command conducted a recent, detailed analysis. [redacted]. Therefore, we request that the Commander, USCENTCOM reconsider his position and provide additional comments on the final report by January 8, 2015.

(U) Management Comments Required

(U) The Commanders, USPACOM; U.S. European Command; U.S. Southern Command; U.S. Special Operations Command; U.S. Transportation Command; USSTRATCOM; U.S. Northern Command; and U.S. Africa Command did not respond to the recommendation on the report. We request that the commanders provide comments on the final report by January 8, 2015.

(U) Recommendation 3

(U) We recommend that the Commanders, U.S. Strategic Command and U.S. Cyber Command

(U) USCYBERCOM Comments

~~(S//REL TO USA, FVEY)~~ The Deputy Commander, USCYBERCOM, responding for the Commander, USCYBERCOM,

. In particular, the Deputy Commander stated that USCYBERCOM

Although the Deputy Commander agreed that the

~~(S//REL TO USA, FVEY)~~

CENTCOM (b)(1), 1.4(g). CYBERCOM, (b)(1), 1.4(a).

(U) Our Response

~~(S//REL TO USA, FVEY)~~ Comments from the Deputy Commander partially addressed the specifics of the recommendation.

CENTCOM, (b)(1), 1.4(g).

1.4(a), 1.4(e).

~~(S//REL TO USA, FVEY)~~

~~(S//REL TO USA, FVEY)~~

Finding

(~~S//REL TO USA, FVEY~~) We disagree that actions to [redacted]. Therefore, we request that the Commander, USCYBERCOM reconsider his position, and provide additional comments on the final report by January 8, 2015.

(U) Unsolicited Management Comments

(U) Cost Assessment and Program Evaluation Comments

(U) Although not required to comment, the Director, Cost Assessment and Program Evaluation, stated that DoD was reviewing cyber resource issues for FY 2016 through FY 2020 as part of its annual Program and Budget Review. The Director also stated that the DoD OIG findings about JCC and CSE resourcing needs would be included as part of that review.

(U) Our Response

(U) We commend DoD for reviewing JCC and CSE manpower needs as part of the future budget process in light of competing requirements in a resource-constrained environment. The results of the review could support DoD's ability to resolve our concerns and enable the Combatant Commands, the Service Components, and USCYBERCOM to effectively meet future cyberspace requirements.

(U) Joint Staff Comments

(U//~~FOUO~~) Although not required to comment, the Vice Director, Joint Staff, responding for the Director, Joint Staff, agreed with the report but recommended revisions to align with [redacted].

(U) Our Response

(U//~~FOUO~~) We recognize the 2013 Execute Order requires USSTRATCOM to provide [redacted]

(U//~~FOUO~~) Combatant Command. We understand the constraints on USCYBERCOM and USSTRATCOM [redacted]. Therefore, it is essential for USCYBERCOM and USSTRATCOM to begin [redacted] just the liaison officer position that is now currently staffed [redacted]. By continuing to make exceptions for providing CSE functionality at the commands as training and manpower allowed, [redacted]

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from December 2013 through September 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We visited Headquarters, USPACOM, Camp H.M. Smith, Hawaii, and Headquarters, USCENTCOM, MacDill Air Force Base, Florida. We interviewed officials from the JCCs and other joint directorates at USPACOM and at USCENTCOM to determine how the commands:

- (U) established and resourced the JCCs;
- (U) identified and completed Joint Staff–directed tasks and other command cyberspace priorities;
- (U//~~FOUO~~) integrated cyberspace capabilities into operational and contingency plans; and
- (U//~~FOUO~~) [redacted].

(U//~~FOUO~~) In addition, we interviewed the CSEs at both commands to determine how they completed Joint Staff–directed tasks and supported the JCCs in planning and integrating cyberspace into operations. At USPACOM, we also met with the Director, J6 and the Director, J2 to discuss their plans for building and sustaining cyberspace capabilities and supporting the Commander, USPACOM's cyberspace missions and responsibilities in the theater.

(U//~~FOUO~~) We obtained [redacted]; memorandums of agreement with USCYBERCOM for CSE support; external manpower assessments related to the organizational missions of each command; integrated priority lists from each command identifying its cyberspace

(U//~~FOUO~~) priorities [redacted]; the USPACOM initial operating capability message and the USCENTCOM JCC charter; and internal assessments about their abilities to complete the cyberspace tasks directed by the Joint Staff.

(U) We visited Headquarters, Fleet Cyber Command, Fort Meade, Maryland, and interviewed officials to determine the command's responsibilities for supporting USPACOM cyberspace operations at its Joint Force Headquarters–Cyber. We also visited Headquarters, USCYBERCOM, Fort Meade, Maryland, and interviewed officials responsible for planning and directing cyberspace operations and fielding the Cyber Mission Forces. We also met with the Chief of Staff and the Director, J8 (Capability and Resource Integration Directorate) to discuss their visions on how the Cyber Mission Forces would be used in DoD, USCYBERCOM's support of combatant commanders cyberspace operations, and USCYBERCOM's efforts to fill CSEs at the Combatant Commands.

(U//~~FOUO~~) We obtained and reviewed USCYBERCOM manpower-issue papers and its [redacted]; Deputy Secretary of Defense memorandums, "Resource Management Decisions for the FY 2014 Budget Request," April 10, 2013, and "Resource Management Decisions for the FY 2015 Budget Request," March 6, 2014, to determine USCYBERCOM, USPACOM, and USCENTCOM authorized and funded manpower for implementing the Transitional Cyberspace Operations C2 Concept of Operations; [redacted]; and proposed guidance (concept of operations) for employing Cyber Mission Forces [redacted].

(U//~~FOUO~~) We interviewed officials from the Joint Staff to determine their responsibilities in coordinating and issuing cyberspace requirements, [redacted]. We obtained and reviewed the Transitional Cyberspace Operations C2 Concept of Operations to identify USCYBERCOM and combatant commanders' responsibilities for planning, integrating, synchronizing, and deconflicting cyberspace operations; a 2012 Air Force Personnel Center Manpower Directorate study [redacted]; combatant commander's submissions [redacted]; and the June 21, 2013, Execute Order to determine specific requirements for building a C2 of

(U//~~FOUO~~) cyberspace operations construct. We also visited the Joint Staff J7 in Suffolk, Virginia, and interviewed officials from the Joint and Coalition Operational Analysis team to determine their scope, methodology, and results from the year-long study from 2012 through 2013 of DoD's progress in implementing the Transitional Cyberspace Operations C2 Concept of Operations.

(U) We also interviewed officials from the Offices of the Chief Information Officer and the Deputy Assistant Secretary of Defense for Cyber Policy and the Director, Command, Control, Communications, and Computers and Information Programs Division, Cost Assessment and Program Evaluation to determine their responsibilities in issuing policy and guidance affecting cyberspace operations and cyber workforce development and training, and reviewing combatant commander issue papers related to JMVP requests. Furthermore, we interviewed officials from Headquarters, Defense Information Systems Agency to determine their responsibilities in supporting USCYBERCOM and combatant commanders' abilities to conduct defensive and DoDIN operations. We also interviewed officials from the Defense Information Systems Agency–Pacific to determine how the agency supported USPACOM's defensive and DoDIN operations in the theater.

(U) We also obtained and reviewed security classification guides from USPACOM, USCENTCOM, USCYBERCOM, and the Defense Information Systems Agency, to appropriately classify information and portion mark the report.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this audit.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) issued five reports discussing issues affecting Combatant Command's abilities to resource and conduct cyberspace operations. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov.

(U) GAO

(U) Report No. 13-293, "DoD Needs to Periodically Review and Improve Visibility of Combatant Commands' Resources," May 15, 2013

(U) Report No. 12-8, "Initiatives Need Better Planning and Coordination," November 29, 2011

(U) Report No. 11-75, "DoD Faces Challenges in its Cyber Activities," July 25, 2011

(U) Report No. 11-421, "More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 20, 2011

~~(S)~~ Report No. 10-479C, "DoD Faces Challenges in its Cyber Efforts," May 20, 2010

(U) Appendix B

(U) Key Cyberspace Events

(U) Figure B below identifies key events affecting combatant commander cyberspace operations from March 2012 through June 2014.

(S//REL TO USA, FVEY) Figure B. Key Events Affecting Combatant Command Cyberspace Operations

(U) Source: [illegible]

(U) Appendix C

(U) Cyberspace Tasks Directed by Joint Staff

(U) Table C below lists the 65 (41 JCC and 24 geographic Combatant Command) cyberspace tasks directed by the Joint Staff and prescribed in the March 15, 2012, Transitional Cyberspace Operations C2 Concept of Operations. [redacted]

(S) Table C. Cyberspace Tasks Directed by Joint Staff and Status of Completion

Joint Staff Cyberspace Tasks	Status of Completion USPACOM (as of June 2014)	Status of Completion USCENTCOM (as of February 2013)
JCC Tasks		
[redacted]		

~~SECRET~~

Appendixes

SECRET Joint Staff Cyberspace Tasks	Status of Completion USPACOM (as of June 2014)	 USCENTCOM (as of February 2013)
CENTCOM (b)(1) 1.4(g); CYBERCOM; (b)(1) 1.4(a); OSD/JS (b)(1), 1.4(a), 1.4(e), 1.4(g); PACOM (b)(1), 1.4(a), 1.4(e) 1.4(g)		

~~SECRET~~

~~SECRET~~

Joint Staff Cyberspace Tasks	Status of Completion	
	USPACOM (as of June 2014)	USCENTCOM (as of February 2013)

ENTCOM, (b) (1), 1.4(g); CYBERCOM; (b) (1), 1.4(a), OSD/JS; (b) (1), 1.4(a), 1.4(c), 1.4(g), PACOM, (b) (1), 1.4(a), 1.4(e) 1.4(g)

~~SECRET~~

Appendixes

SECRET Joint Staff Cyberspace Tasks	Status of Completion USPACOM (as of June 2014)	 USCENTCOM (as of February 2013)
CENTCOM: (b) (1), 1.4(g), CYBERCOM: (b) (1), 1.4(a), OSD/JS: (b) (1), 1.4(a), 1.4(e), 1.4(g), PACOM: (b) (1), 1.4(a), 1.4(e), 1.4(g)		

SECRET

~~SECRET~~

Joint Staff Cyberspace Tasks	Status of Completion	
	USPACOM (as of June 2014)	USCENTCOM (as of February 2013)

ENTCOM; (b) (1), 1.4(g), CYBERCOM (b) (1), 1.4(a), OSD/JS. (b) (1), 1.4(a), 1.4(e), 1.4(g), PACOM. (b) (1), 1.4(a), 1.4(e), 1.4(g)

~~SECRET~~

Appendixes

Joint Staff Cyberspace Tasks	Status of Completion	
	USPACOM (as of June 2014)	USCENTCOM (as of February 2013)
CENTCOM: (b)(1), 1.4(g); CYBERCOM: (b)(1), 1.4(a); OSD/JS: (b)(1), 1.4(a), 1.4(c), 1.4(g); PACOM: (b)(1), 1.4(a), 1.4(e), 1.4(g)		

~~SECRET~~

(U) Management Comments

(U) U.S. Central Command

Final Report Reference

SECRET//NOFORN

UNITED STATES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

8 October 2014

MEMORANDUM FOR DOD OFFICE OF THE INSPECTOR GENERAL

SUBJECT: (U//FOUO) Joint Cyber Center [redacted] Cyberspace Operations (U//FOUO)

References: (a) (JSAP; SJS 14-04027 (S))
(b) (IG Report, Project No. D2014-D000RC-0074.000 (S//NF))

1. (U) The IG's objective was to determine whether Combatant Commands [redacted] from U.S. Cyber command (USCYBERCOM) to effectively conduct cyber operations in their areas of operations.

2. (U//[redacted] The findings resulted in USCENTCOM [redacted] in its Joint Cyber Center and Cyber Support Element (CSE) support for USCYBERCOM to fully perform the essential cyberspace tasks directed by the Joint Staff for planning, integrating and synchronizing cyberspace operations.

3. (U) Recommendation: The IG recommends that all combatant commanders conduct a command-wide, mi[redacted] Furthermore, the IG recommends that the Commander's [redacted] Command and USCYBERCOM [redacted] — Recommendation 2, Revised

4. (U) J1 concurs with the IG findings as stated in the report. The IG's recommendation to conduct a command-wide mission-[redacted]ted at USCENTCOM internally by the USCENTCOM JC[redacted] Additionally, the [redacted]

[redacted]

Chief, Manpower Division

Classified by: [redacted]
Derived From: Multiple Sources
Declassify on: September 1, 2019

SECRET//NOFORN

(U) U.S. Cyber Command

Final Report Reference

DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

23 October 2014

Reply to:
Commander

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Through: Vice Chairman, Joint Chiefs Of Staff

Subject: (U) United States Cyber Command's (USCYBERCOM) Support to Combatant Commands (CCMDs)

Reference: DoDIG Report - Project No. DJO14-D000RC-0074.000

1. (U) USCYBERCOM appreciates the opportunity to review the DoDIG report, referenced above, regarding USCYBERCOM's support to CCMDs. As the report cites, USCYBERCOM has exercised every feasible course of action to provide cyber support element (CSE) support to the CCMDs, including

[redacted] CENTCOM (b)(1), 1.7(e), DoD OIG (b)(7)(E)

b. (U) Planning validation of the [redacted] DoD OIG (b)(7)(E) [redacted] were [FY13 and FY14]. In accordance with the DoD approved Joint Manpower Validation Process. Although the [redacted] CENT billets were validated twice, they were never sourced.

[redacted] with the findings that [redacted] CENTCOM (b)(1), 1.7(e), DoD [redacted] cyberspace operations. However, we disagree with the recommended [redacted] USCYBERCOM to [redacted] CENTCOM (b)(1), 1.7(e), DoD OIG (b)(7)(E) [redacted] CENTCOM (b)(1), 1.7(e), DoD OIG (b)(7)(E)

Recommendation 3, Revised

Derived from: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20390501

[redacted]

(U) U.S. Cyber Command (cont'd)

[redacted]

[redacted]

5. (U) As discussed above, due to the lack of sufficient authorizations to achieve IOC, additional mission already absorbed using existing manpower, and the pending DepSecDef-directed comprehensive manpower assessment, it would be inappropriate to immediately implement the recommendation as written. However, we will address the findings and recommendations during the comprehensive manpower assessment to ensure all receive appropriate consideration.

6. (U) The J7/SCYBERCOM point of contact for this action is [redacted]

Kevin S. Laughlin
Lieutenant General, U.S. Air Force
Deputy Commander

Copy to:
Commander, USSTRATCOM

[redacted]

Management Comments

(U) Joint Staff

Final Report Reference

UNCLASSIFIED//[redacted]

THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-0300

DJSM-1034-14
6 November 2014

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: [redacted] Cyberspace Operations
(Project No. D2014-D000JB-0074.000)

1. (U//[redacted]) Thank you for the opportunity to review and comment on the subject report. The Joint Staff concurs with the report and offers one comment.

[redacted]

Revised

(U) We recommend that the Commanders, U.S. Strategic Command and U.S. Cyber Command increase Cyber Support Element support to all Combatant Commands as manpower and training allow and develop alternative solutions for sustaining forward-deployed Cyber Support Elements to directly support Combatant Commands in planning and integrating cyberspace capabilities into operations.

3. (U) The Joint Staff point of contact [redacted]

FREDERICK S. RUDESHEIM
Major General, USA
Vice Director, Joint Staff

UNCLASSIFIED//[redacted]

(U) Cost Assessment and Program Evaluation

OFFICE OF THE SECRETARY OF DEFENSE
1800 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1800

COST ASSESSMENT AND PROGRAM EVALUATION

NOV 3 2014

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Draft DoD Inspector General (IG) Report on Joint Cyber Centers

Thank you for the opportunity to review the draft DoD IG report on Command [redacted] Cyberspace Operations." My staff reviewed the findings and recommendations in the report and found them to be useful.

As the draft report correctly points out, the Department must prioritize competing requirements in a resource-constrained environment. The DoD is currently performing its annual Program and Budget Review, which will include reviewing issues related to cyber resources for Fiscal Years 2016-2020. Although this information is pre-decisional and cannot be shared until the President's Budget has been submitted to Congress, we will take into consideration the findings in the draft DoD IG report as we review any issues relating to Joint Cyber Centers or Cyber Support Elements.

I concur with the findings as written in the draft report, but defer commenting on the recommendations in the draft report until the Department has completed its Program and Budget Review process for Fiscal Years 2016-2020. My point of contact for this work is [redacted]

Jamie M. Morin
Director

(U) Source of Classified Information

Source 1: (U) Department of Defense Strategy for Operating in Cyberspace: S//REL TO USA, FVEY

Declassified Date: May 26, 2036

Generated Date: May 2011

Source 2: ~~(S//REL TO USA, FVEY)~~ Joint Publication 3-12, "Cyberspace Operations"

Declassified Date: September 25, 2034

Generated Date: February 5, 2013

Source 3: ~~(S//REL TO USA, AUS, CAN, GBR)~~ U.S. Cyber Command Cyber Force Concept of Operations, Version 3.4

Declassified Date: November 20, 2038

Generated Date: March 31, 2014

Source 4: ~~(S//REL TO USA, FVEY)~~ [redacted]

Declassified Date: June 22, 2038

Generated Date: June 21, 2013

Source 5: (U) Cyber Mission Force: Concept of Operations: S//REL TO USA, FVEY

Declassified Date: December 11, 2037

Generated Date: January 16, 2014

Source 6: ~~(S//REL TO USA, FVEY)~~ FY 2014 – 2016 Cyber Mission Force Fielding Timeline

Declassified Date: May 1, 2039

Generated Date: Undated

Source 7: ~~(S)~~ Cyber Pacific Task Crosswalk – All 259 Tasks

Declassified Date: June 28, 2039

Generated Date: June 30, 2014

Source 8: ~~(S//NF)~~ JCC Joint Manpower Validation Board

Declassified Date: August 14, 2038

Generated Date: August 14, 2013

Source 9: (U) Transitional Cyberspace Operations C2 Concept of Operations Study Report: S//NF

Declassified Date: July 15, 2038

Generated Date: July 15, 2013

Source 10: ~~(S)~~ Email from [redacted] Concerning U.S. Northern Command's Requests for Manpower for PBR16

Declassified Date: Undated

Generated Date: June 3, 2014

Source 11: ~~(S//REL TO USA, FVEY)~~ USPACOM CSE Binder

Declassified Date: June 22, 2038

Generated Date: Undated

Source 12: ~~(S//REL TO USA, FVEY)~~ [redacted]

Declassified Date: June 12, 2037

Generated Date: June 12, 2012

Source 13: ~~(S//REL TO USA, FVEY)~~ [redacted]

Declassified Date: June 18, 2037

Generated Date: June 18, 2012

Source 14: ~~(S//REL TO USA, FVEY)~~ Air Force Cyber Command Reclama on USCYBERCOM Task Order 12-1387 for USPACOM CSE Personnel Sourcing

Declassified Date: December 12, 2037

Generated Date: December 12, 2012

Source of Classified Information

Source 15: ~~(S//REL TO USA, FVEY)~~ Army Cyber Command Request for Relief of Tasking for USPACOM CSE Personnel

Declassified Date: May 15, 2038

Generated Date: May 15, 2013

Source 16: ~~(S//REL TO USA, FVEY)~~ Fleet Cyber Command USPACOM CSE Personnel Support Reclama

Declassified Date: October 1, 2038

Generated Date: October 1, 2013

Source 17: ~~(S//NF)~~ Deputy Under Secretary of Defense for Joint and Coalition Warfighter Support Action Memo, FY 2014-2018 Joint Manpower Validation for Military Intelligence Program Requirements

Declassified Date: July 20, 2037

Generated Date: July 20, 2012

Source 18: (U) Email from DoD OIG; (b) (6), CYBERCOM; (b) (3), 10 USC § 130b Containing USCYBERCOM Manpower Documentation: S//NF

Declassified Date: February 3, 2039

Generated Date: February 3, 2014

Source 19: (U) USCYBERCOM Manpower Brief to the DoD IG Audit Team: S//REL TO USA, FVEY

Declassified Date: May 7, 2038

Generated Date: January 15, 2014

Source 20: ~~(S//REL TO USA, FVEY)~~ USCYBERCOM Task Order 13-0747, Establishment and Presentation of Cyber Mission Force Teams in FY 2014

Declassified Date: October 11, 2038

Generated Date: October 11, 2013

Source 21: ~~(S//REL TO USA, FVEY)~~ CSE Manpower In Support of USPACOM Cyber Pacific

Declassified Date: Undated

Generated Date: January 18, 2014

Source 22: (U) USCYBERCOM Briefing from Chief, Plans Division: S//NF

Declassified Date: May 10, 2038

Generated Date: Undated

Source 23: ~~(S)~~ Email from [redacted] Regarding USPACOM Plans

Declassified Date: June 25, 2024

Generated Date: June 25, 2014

Source 24: ~~(S//REL TO USA, FVEY)~~ USCENTCOM Responses to OIG Follow up

Declassified Date: March 3, 2024

Generated Date: June 9, 2014

Source 25: (U) Transitional Cyberspace Operations C2 Concept of Operations Study Final Brief: S//NF

Declassified Date: July 15, 2038

Generated Date: July 15, 2013

Source 26: ~~(S)~~ 2014 U.S. Africa Command JMVP Request

Declassified Date: Undated

Generated Date: May 27, 2014

Source 27: (U) U.S. Special Operations Command JMVP Submission for FY 2016 President's Budget Request: S

Declassified Date: February 11, 2038

Generated Date: May 29, 2014

Source 28: ~~(S//NF)~~ USPACOM JCC Manpower Issue Paper Submitted to Office of the Secretary of Defense Cost Assessment and Program Evaluation

Declassified Date: November 19, 2038

Generated Date: November 20, 2013

Source 29: ~~(S)~~ [redacted]

Declassified Date: September 27, 2023

Generated Date: Undated

Source of Classified Information

Source 30: ~~(S//NF)~~ USCENTCOM Capability Gap Analysis

Declassified Date: March 3, 2024

Generated Date: Undated

Source 31: ~~(S)~~ Cyber Pacific Task Crosswalk Assessments with Mission Capability and Task Attribution- Transitional Cyberspace Operations C2 Concept of Operations Only

Declassified Date: April 30, 2039

Generated Date: June 13, 2014

Source 32: (U//~~FOUO~~) Response to DoD IG Inquiry: Cyber Pacific Task Analysis Letter: S

Declassified Date: June 6, 2024

Generated Date: June 6, 2014

Source 33: ~~(S//REL TO USA, ACGU~~) Extract from the Commander, USCENTCOM Integrated Priority List, Priority 7, USCENTCOM Full Spectrum Cyberspace Operations

Declassified Date: March 3, 2024

Generated Date: Undated

Source 34: (U) USCENTCOM Science and Technology Integrated Priority List Synopsis for Supporting Requirements for 11 of the FY 16-20 Integrated Priority Lists: S//NF

Declassified Date: April 10, 2024

Generated Date: Undated

Source 35: (U) USCENTCOM 2014 Science and Technology Support Requirements: S//NF

Declassified Date: April 10, 2014

Generated Date: April 10, 2014

Source 36: ~~(S//REL TO USA, FVEY)~~ [redacted]

Declassified Date: October 4, 2038

Generated Date: October 4, 2013

Source 37: ~~(S//REL TO USA, FVEY)~~ USCENTCOM JCC Charter

Declassified Date: February 22, 2038

Generated Date: March 14, 2013

Source 38: (U) Operations Deputies Tank Review of USCYBERCOM Manpower Request: S

Declassified Date: July 1, 2037

Generated Date: July 25, 2012

Source 39: (U) Resource Management Decisions for the FY 2014 Budget Request: S//NF

Declassified Date: April 10, 2038

Generated Date: April 10, 2013

Source 40: (U) Resource Management Decisions for the FY 2015 Budget Request: S//NF

Declassified Date: March 6, 2039

Generated Date: March 6, 2014

Source 41: ~~(S//REL TO USA, FVEY)~~ USCENTCOM CSE Personnel Support Reclama from Commander, Fleet Cyber Command

Declassified Date: October 1, 2038

Generated Date: October 1, 2013

Source 42: ~~(S)~~ USCYBERCOM Instruction 5200.07, Cyber Mission Forces Security Classification Guide

Declassified Date: September 1, 2023

Generated Date: November 26, 2013

Source 43: (U) Government Accountability Office Report GAO-10-479C, DoD Faces Challenges in Its Cyber Efforts: S

Declassified Date: May 6, 2020

Generated Date: May 2010

(U) Acronyms and Abbreviations

C2	Command and Control
CSE	Cyber Support Element
DoDIN	DoD Information Network
JCC	Joint Cyber Center
JMVP	Joint Manpower Validation Process
USCENTCOM	U.S. Central Command
USCYBERCOM	U.S. Cyber Command
USPACOM	U.S. Pacific Command
USSTRATCOM	U.S. Strategic Command

~~SECRET//NOFORN~~

Whistleblower Protection

U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098